REMARKS

This Application has been carefully reviewed in light of the Office Action mailed April 21, 2005. Claims 1-23 were pending in the Application. In the Office Action, Claims 1-23 were rejected. Claims 1-23 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

DOUBLE PATENTING REJECTION

Claims 1-8, 9-18 and 20-23 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-8, 10-19, and 21-24 of co-pending Application No. 10/001,350. In this regard, the Examiner states that "[a]lthough the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the referenced copending [sic] application" (Office Action, page 2) (emphasis added). Applicants respectfully traverse this provisional rejection.

Applicants respectfully remind the Examiner that for an obviousness-type double patenting rejecting, the disclosure of the co-pending application may not be used as prior art against the claims of the instant application. *See* M.P.E.P. § 804(II)(B)(1). Independent Claim 1 of the instant application, for example, recites "retrieving an web browser-based template" and "graphically displaying the correlated decoded data components using the web browser-based template." At least the above-referenced limitations of independent Claim 1 of the instant application are not recited by the claims of the co-pending application. However, the Examiner has not provided any basis or reasoning as to why the Examiner considers the claims of the instant application an obvious variation of the invention defined by a claim of the co-pending application, which is required to support an obviousness-type double patenting rejecting. *See* M.P.E.P. § 804(II)(B)(1)(a). Nor has the Examiner provided any such reasoning for remaining rejected Claims 2-8, 9-18 and 20-23 of the instant application. To the contrary, the Examiner appears to reject the claims of the instant

application based solely on the disclosure of the co-pending application, which is improper. Accordingly, for at least this reason, the rejection is improper and should be withdrawn.

SPECIFICATION OBJECTIONS

The specification was objected to for informalities. The Examiner suggested that Applicants provide the serial numbers of all co-pending applications mentioned on pages 1-2 of the disclosure and page 7. Applicants have amended pages 1-2 and 7 of the specification to include the serial numbers of the respective noted co-pending applications. Accordingly, Applicants respectfully request that the specification objections be withdrawn.

DRAWING OBJECTIONS

The drawings were objected to as failing to comply with 37 CFR §1.84(p)(4). Specifically, the Examiner indicated that reference character "18" was used to designate both "storage device or database" in FIGURE 1 and "HTML" in FIGURE 2. Applicants respectfully disagree. Applicants' specification, referring to FIGURE 1, recites: "A storage device or database (DB) 18 storing a variety of information is accessible by intrusion protection system 14" (page 5, lines 18-20, FIGURE 1). In FIGURE 2 of Applicants' specification, Applicants respectfully submit that reference numeral 18 is used to generally refer to such a database (e.g., by indication with an arrowhead and being offset or not directly contacting any element in FIGURE 2) where, in FIGURE 2, such a database 18 comprises HTML templates 30. Thus, Applicants respectfully submit that Applicants' use of reference numeral 18 in FIGURES 1 and 2 is proper, and request that this drawing objection be withdrawn.

The Examiner also objected to the drawings as failing to comply with 37 CFR 1.84(p)(5) because the reference character 124 in FIGURE 5 was not mentioned in the description. Applicants have amended FIGURE 5 to remove reference numeral 124. A replacement sheet of the drawing containing amended FIGURE 5 is attached herewith in Appendix A. Applicants respectfully request that this drawing objection be withdrawn.

SECTION 101 REJECTIONS

Claims 1-23 were rejected under 35 U.S.C. §101 as being directed to non-statutory matter. Applicants respectfully traverse this rejection.

In the Office Action, the Examiner appears to assert that because Claims 1, 9 and 16 recite "decipherable by humans," such claims are directed to non-statutory subject matter (Office Action, page 5). Applicants respectfully disagree. Applicants respectfully refer the Examiner to M.P.E.P. § 2106(IV)(B)(2)(a) which recites that "[o]ffice personnel must treat each claim as a whole" (emphasis added). Further, a claim is limited to a practical application, and is therefore statutory, when the method, as claimed, produces a concrete, tangible and useful result. M.P.E.P. § 2106(IV)(B)(2)(b)(ii). Applicants respectfully submit that independent Claims 1, 9 and 16, when evaluated as a whole, produce a concrete, tangible and useful result and, therefore, are statutory. For example, independent Claim 1 is directed toward a "method of displaying data related to an intrusion event on a computer system" comprising "capturing data related to the intrusion event," "decoding the captured data," "correlating data components of the intrusion signature, data summary and detailed data to one another," "retrieving an web browser-based template" and "graphically displaying the correlated decoded data components using the web browser-based template." Thus, independent Claim 1 is clearly producing a concrete, tangible and useful result and, therefore, is statutory. Independent Claims 9 and 16 recite similar limitations that also produce a concrete, tangible and useful result.

Moreover, even when the portion of Claims 1, 9 and 16 referred to by the Examiner is viewed in isolation, which Applicants submit is improper, such portion, by itself, produces a concrete, tangible and useful result. For example, Claim 1 recites "decoding [captured data related to an intrusion event] from a first predetermined format to a second predetermined format decipherable by humans" (e.g., decoding from a machine-readable format to a human-readable format). Accordingly, Claims 1, 9 and 16, and Claims 2-8, 10-15 and 17-23 that depend respectively therefrom, are directed toward patentable subject matter. Therefore, Applicants respectfully request that this rejection be withdrawn.

SECTION 103 REJECTIONS

Claims 1, 5-9, 12-16 and 19-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,269,447 issued to Maloney et al. (hereinafter "*Maloney*") and further in view of U.S. Publication No. 2004/0103315 issued to Cooper et al. (hereinafter "*Cooper*"). Claims 2-4, 10-11 and 17-18 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Maloney* and *Cooper* as applied to claims 1 and 9 and further in view of U.S. Patent No. 6,775,583 issued to Slodowski et al. (hereinafter "*Slodowski*"). Applicants respectfully traverse these rejections.

Of the rejected claims, Claims 1, 9 and 16 are independent. Applicants respectfully submit that neither *Maloney* nor *Cooper*, alone or in combination, discloses, teaches or suggests the limitations of independent Claims 1, 9 and 16. For example, in the Office Action, the Examiner refers to column 4, lines 34-40, of *Maloney* as disclosing "decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans" as recited by independent Claim 1 (Office Action, page 6). Applicants respectfully disagree. Column 4, lines 34-40, of *Maloney* appears to recite that "[d]ata in the knowledge base 16 is made available to a data parsing tool 18 that converts the captured network data from the discovery tool 12 to a form useable by downstream programs of the system" (emphasis added). Thus, Applicants respectfully submit that the portion of *Maloney* referred to by the Examiner does not appear to disclose or even suggest "decoding the captured data [related to an intrusion event] from a first predetermined format to a second predetermined format decipherable by humans" as recited by independent Claim 1 (emphasis added). Further, *Cooper* does not appear to remedy at least this deficiency of *Maloney*. Accordingly, for at least this reason, independent Claim 1 is patentable over the proposed combination of references.

Additionally, independent Claim 1 recites "decoding the captured data [related to an intrusion event] . . . the decoded data comprising data components of intrusion signature, data summary, and detailed data" and "correlating data components of the intrusion signature, data summary and detailed data to one another" (emphasis added). In the Office Action, the Examiner refers to column 4, lines 34-40 and 53-60, of *Maloney* as disclosing the above-

referenced limitations of independent Claim 1 (Office Action, page 6). Applicants respectfully disagree. *Maloney* appears to disclose a discovery tool 12 that "collects traffic and usage data" which becomes part of the knowledge base 16 of *Maloney* (*Maloney*, column 4, lines 23-26) (emphasis added). *Maloney* also appears to disclose that data in the knowledge base 16 of *Maloney* is accessed by a parsing tool 18 and made available to an analytical engine 20 for analyzing the data captured by the discovery tool 12 and for developing and comparing network usage patterns (*Maloney*, column 4, lines 34-41). *Maloney* also recites :

> After collecting and organizing data, the analytical engine 20 can be used to make associations between a number of different data charts to determine correlation and differentiation. Relationships between an array of data sources are then available to verify hypothesis, to correlate relationships among multiple data sets and to identify target data within a large data set. Network data needs to be analyzed in order to relate knowledge base data to session data, packet data, and alert data. These relationships assist in determining who has been talking to whom, as well as the content of the traffic for specific protocols . . . . In the process of analyzing network data, a determination is made as to what IP and/or MAC addresses are common to more than one data set. . . . The average of what IP and MAC addresses exist are used to create a link chart representing traffic between each address set.

(*Maloney*, column 4, lines 54-67, column 5, lines 1-4). Thus, *Maloney* does not appear to disclose or even suggest, in the portion of *Maloney* referred to by the Examiner or elsewhere in *Maloney*, that the data decoded by the *Maloney* system includes "data components of [an] intrusion signature" as recited by independent Claim 1 (emphasis added). Further, the "correlating" function purportedly performed by the *Maloney* system and referred to by the Examiner in the Office Action appears to directed toward network usage data and patterns, in contrast to "correlating data components of the intrusion signature, data summary and detailed data to one another" as recited by independent Claim 1 (emphasis added). In fact, the Examiner does not appear to explicitly identify any disclosure in *Maloney* regarding decoding data related to an intrusion event to obtain "data components of [an] intrusion signature" or "correlating [the] data components of the intrusion signature" to other data as recited by independent Claim 1 (emphasis added). Moreover, *Cooper* does not appear to remedy at least

these deficiencies of *Maloney*. Accordingly, for at least these reasons also, independent Claim 1 is patentable over the cited references.

Independent Claim 9 recites, at least in part, "capturing, from a network, data related to an intrusion event in response to detecting an intrusion signature in the network data," "decoding the captured data from a predetermined format to a human-readable format, the decoded data comprising data components of network header data, data summary, and detailed data" and "determining a correlation relationship between the data components of the intrusion signature, network header data, data summary and detailed data to one another" (emphasis added), and independent Claim 16 recites, at least in part, "a network driver capturing data related to an intrusion event upon detecting a predetermined intrusion signature," "a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising data components of intrusion event data, data summary, and detailed data" and "a user interface graphically correlating data components of the intrusion signature, intrusion event data, data summary and detailed data to one another" (emphasis added). At least for the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that independent Claims 9 and 16 are also patentable over the proposed combination of references. and displaying the correlated decoded data components according to a web browser-based format
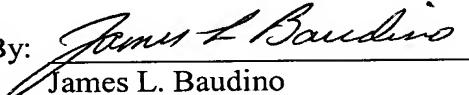
Claims 2-8, 10-15 and 17-23 depend respectively from independent Claims 1, 9 and 16. At least for the reasons discussed above, independent Claims 1, 9 and 16 are in condition for allowance. Therefore, Claims 2-8, 10-15 and 17-23 that depend respectively therefrom are also in condition for allowance. Accordingly, Applicants respectfully request that the rejection of Claims 1-23 be withdrawn.

CONCLUSION

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicants have overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: *James L. Baudino*

James L. Baudino
Reg. No. 43,486

Date: July 19, 2005

Correspondence to:
L.Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
Tel. 970-898-3884

APPENDIX A